Cryptography and Network Security

Multiple Encryption and Triple DES

esoacademy.org

Outcomes

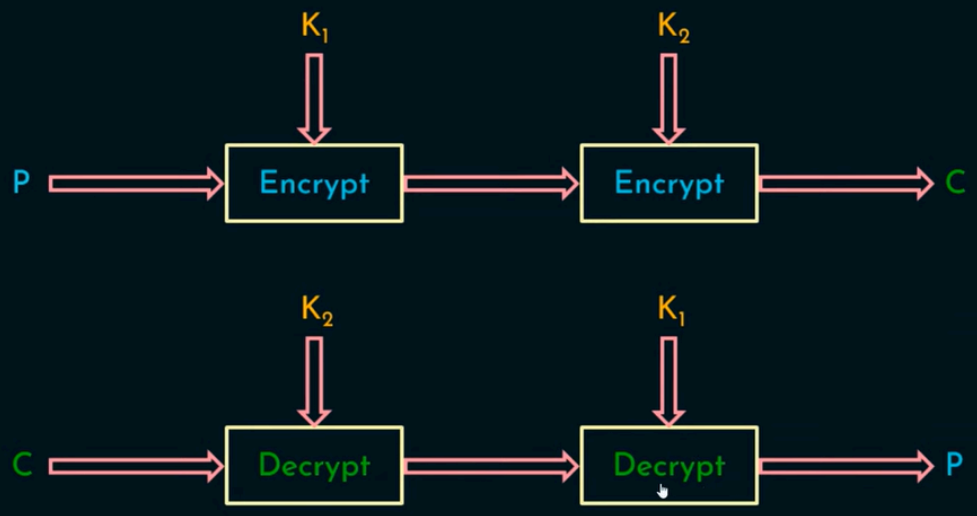
Upon the completion of this session, the learner will be able to

- ★ Understand the drawbacks of DES.
- ★ Know about multiple encryption.
- ★ Know about double DES.
- ★ Know about Meet-in-the-middle (MITM) attack.
- ★ Know about Triple DES.

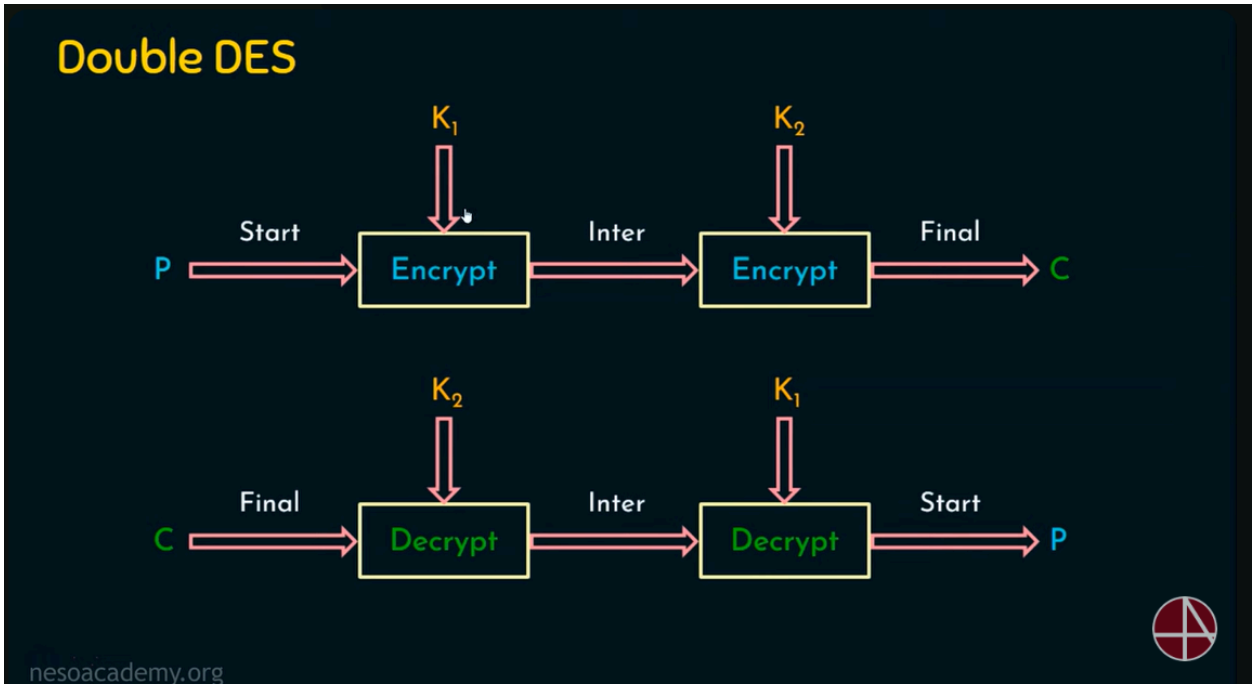
Multiple Encryption and Triple DES

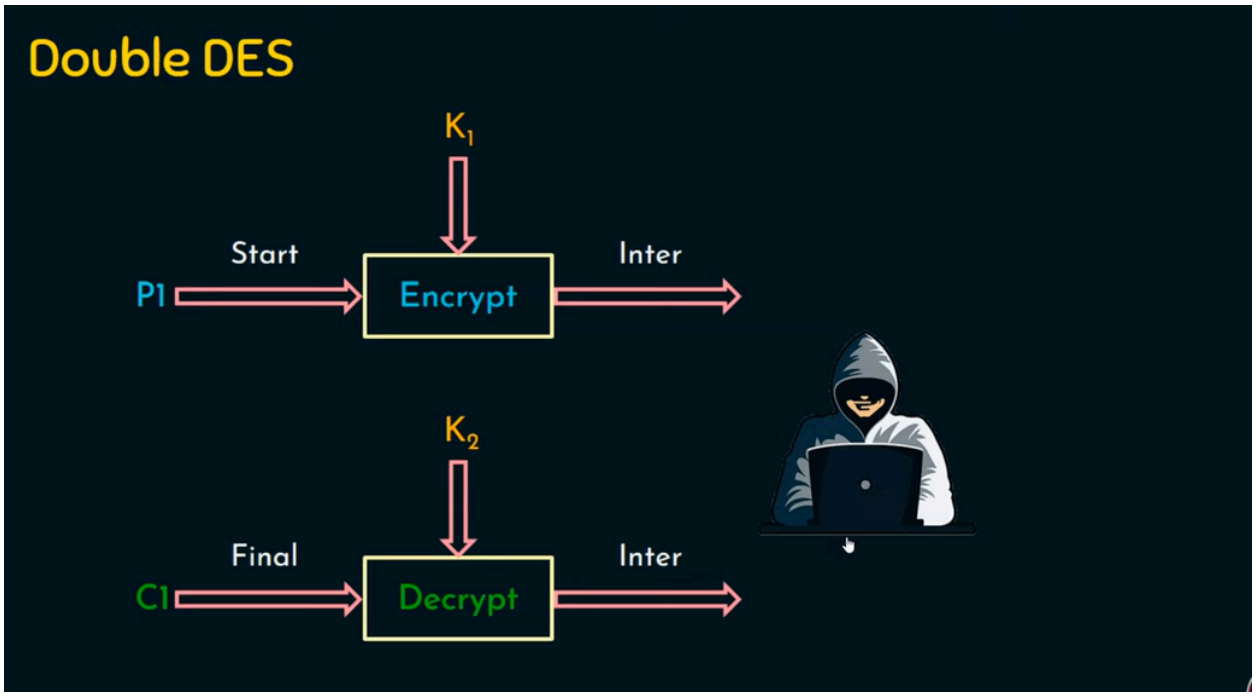
- ★ Drawbacks of DES.
- ★ Potential vulnerability of DES to a brute-force attack.
- ★ AES – Completely a new algorithm.
- ★ Another alternative.
- ★ Use of multiple encryption with DES and multiple keys.

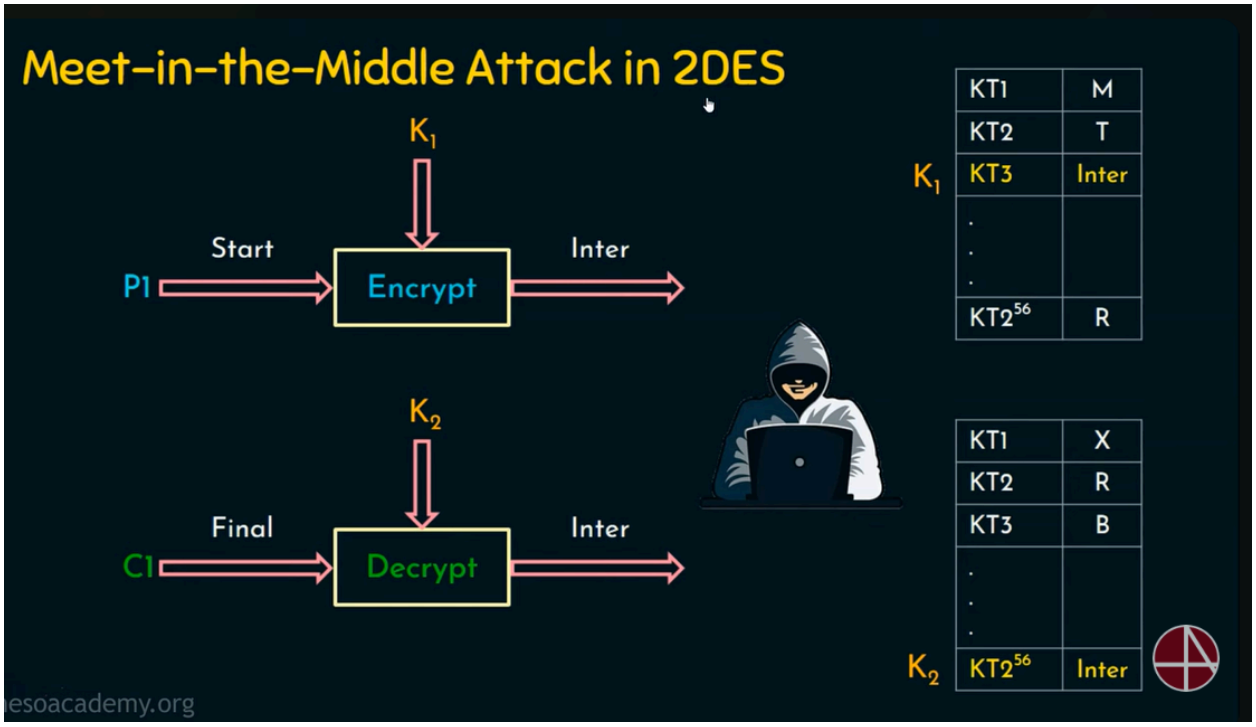
Double DES

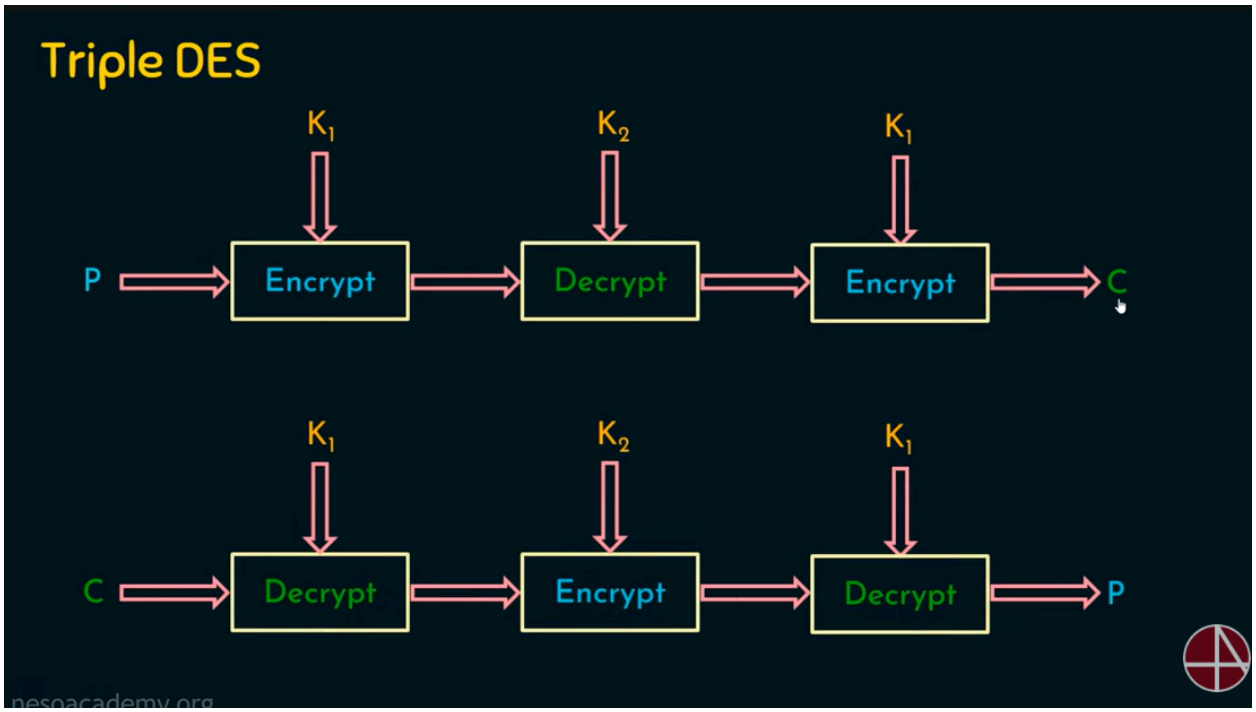


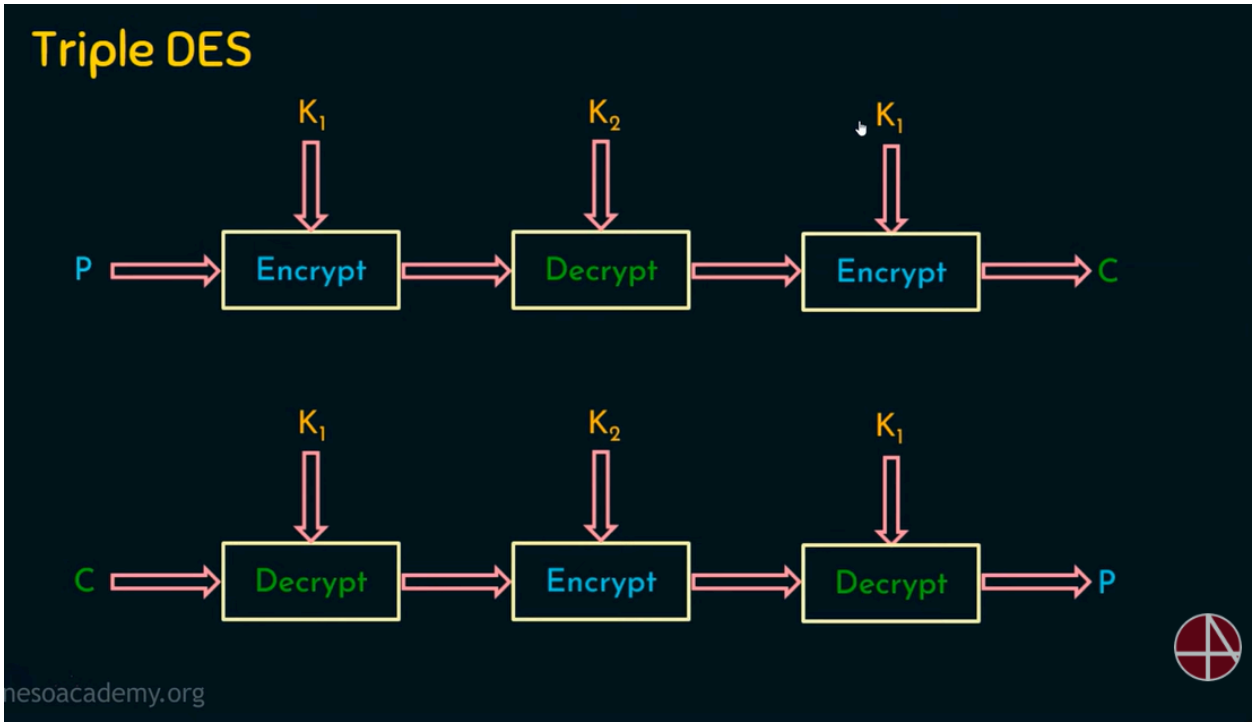
k1!=k2


Double DES
K1
K2
Start
Inter
Final
P
Encrypt
Encrypt
C
K2
K1
Final
Inter
Start
C
Decrypt
Decrypt
P
nesoacademy.org


Double DES
K1
Start
Inter
P1
Encrypt
K2
Final
Inter
C1
Decrypt


Meet-in-the-Middle Attack in 2DES
K1
Start
P1
Encrypt
Inter
K2
Final
C1
Decrypt
Inter
K1
KT1 M
KT2 T
KT3 Inter
KT2^56 R
K2
KT1 X
KT2 R
KT3 B
KT2^56 Inter
esoacademy.org


Triple DES
K1
K2
K1
P
Encrypt
Decrypt
Encrypt
C
K1
K2
K1
C
Decrypt
Encrypt
Decrypt
P
nesoacademy.org


Triple DES
K1
K2
K1
P
Encrypt
Decrypt
Encrypt
C
K1
K2
K1
C
Decrypt
Encrypt
Decrypt
P
nesoacademy.org